Information and Communication Technology

Prins, J.E.J.

Published in:
Netherlands Reports to the Fifthteenth International Congres of Comparative Law

Publication date:
1998

INFORMATION AND COMMUNICATION TECHNOLOGY: AN OVERVIEW OF KEY REGULATORY ISSUES AND STRATEGIES IN THE NETHERLANDS

Corien Prins **VII**
Professor of Law and Informatization, Center for Law, Public Administration and Informatization, Tilburg University, the Netherlands

1 Introduction

Both in Europe and the United States, the development of an information superhighway is seen as vital and indispensable for economic, social and cultural development. Various plans, statements and other documents have been launched, all constituting action frameworks within which a series of relevant policies are articulated to enhance the development of the information superhighway. This attitude is also the one taken by the Dutch government. Reports have been published[1] and an ambitious National Action Programme has been established.[2]

Since, at a worldwide level, the first of the various policy documents appeared, numerous terms have been used to describe the information superhighway: 'Information superhighway', 'global information infrastructure', 'international information infrastructure' (III or Triple-I), 'the national info-communications infrastructure' (Japan), 'data-highway', etc. Whatever it is labelled, it appears that the "information superhighway" has become the holy grail of digitization, dematerialization and interconnectivity. It has developed into the metaphor for a grand vision of our society in which businesses, government bodies, households, schools, and libraries are all linked in a vast web of communication means through which information is exchanged.

With the emergence of this electronic version of physical space, we also find ourselves on the eve of profound legal change. Given the potential applications in an on-line world, we note for example that the traditional difference between text, image and sound – now all digitalized – disappears. Further, with the rise of the electronic information carrier, paper is no longer the medium of choice for exchange of information. Business applications

1. Among which: W.E. Scherpenhuijsen, Visie op versnellen, M&I Partners, Amersfoort 1995 and Diensten en infrastructuren voor elektronische snelwegen in Nederland, M&I Partners, Amersfoort 1996; R. Overdijk, De mythe van de elektronische snelweg: van karrenpad tot snelweg, de ontwikkeling van het elektronisch wegennet, Amsterdam 1997.
2. Actieprogramma Elektronische Snelwegen, Parliamentary Papers, 24 565, no. 1ff.

such as EDI (Electronic Data Interchange) allow computers to ‘decide' and ‘comprehend' without human intervention, thus establishing a contractual relationship. Today, large chain stores no longer require human involvement in stock management, ordering and invoicing. Finally, geographical borders give way to electronic borders in a society where tens of millions of citizens and many thousands of companies are expected to carry out on-line transactions.[3]

Clearly, whatever direction the information superhighway is going to take in the years to come, major legal challenges are bound to appear. It should, however, be noted that these challenges will happen not because no rules apply in an electronically connected environment, but because the traditional rules are irrelevant, problematic, or, at best, ambiguous and unpredictable. One of the principal issues at stake is how to balance the relevant interests in the new digital environment. Legal constraints relating to electronic information services are explicit in the dualism regarding the protection of information (intellectual property rights, privacy rights) on the one hand, and the right to a free flow of information (among which is the right of access to official information), on the other. Having assessed the required balance, we are confronted with the question of how to fit the (desired) consequences into a legal system or alternatively how to achieve the desired legal consequences.

This national report, highlights the principle challenges that appeared or appear under the Dutch legal system as a result of the introduction of information and communication technologies (ICT). Also it discusses the different approaches articulated on how to deal with the challenges. It is beyond the scope of this national report to discuss any of the approaches and developments in detail. The purpose of the paragraphs below is to provide a general overview, offering an insight into the Dutch approach towards ICT regulation.

The report starts with an overview of the principal legal areas affected by electronic communication, thereby concentrating on the Dutch situation. Subsequently, several relevant technology-related developments (smartcard technology, encryption, TTP, etc.) will be discussed. On the basis of this overview, a clearer understanding can be gained of the precise changes and processes that characterise ICT. By looking at the legal consequences of

3. See: S. van der Hof, Online koopovereenkomsten in internationaal privaatrechtelijk perspectief (worktitle); K.R.S.D. Boele-Woelki, “Internet, Consument en IPR: een verkenning”, Consument zonder grenzen, Deventer 1996, pp. 301-313; K.R.S.D. Boele-Woelki, “Internationaal privaatrecht. Internet en IPR”, Ars Aequi Katern 59 1996, pp. 2810-2811.

informatization from the perspective of characteristics and processes and thus clustering these consequences, a better understanding could be gained as to what the impact on the legal system will actually involve. From this perspective, the report discusses the most important views presented on how to regulate information technology developments.

2 Principal legal areas affected by electronic communication

2.1 Criminal Law and Criminal Law Enforcement

In November 1985 a committee was set up by the Ministry of Justice and given the task of investigating whether it was desirable to amend the criminal code and the code of criminal procedure to include certain behaviour characteristics when using computer technology. The committee delivered its report[4] on the basis of which the Minister of Justice published legislative proposals. Finally in 1991, a Computer Crime Act came into force.[5] Interestingly enough, neither the Act nor case law have issued a generally accepted and uniform definition of computer crime. Instead, the earlier-mentioned committee developed a typology.[6]

Since the introduction of the Act many new questions have been discussed, in particular in the light of the arrival of the Internet. Thus, more recently, attention has been drawn to the use of Internet by criminal organizations to transmit pornographic material or discriminatory messages. Questions dealt with in the current studies are: to what extent may certain forms of communication on the Internet be qualified as criminal conduct under the Dutch Criminal Code? What position should the various links (network operators, content providers, etc.) take with respect to possible claims of impunity? Can electronic publishers be prosecuted for transmitting another party's criminal information and remarks? When responding to these questions it is important that the answer must be seen within the framework of the freedom of communication.

A 1996 study concluded that the Dutch Criminal Code “generally shows great elasticity”, meaning that the majority of what is called context-dependent offences (child pornography, discriminatory messages, etc.)

4. Rapport van de commissie computercriminaliteit, Informatietechniek en strafrecht, Staatsuitgeverij, Ministerie van Justitie 1987.
5. Computer Crime Act, Parliamentary Papers 21555, no. 1.ff.
6. See: H.W.K. Kaspersen, “Computer Crimes and Other Crimes against Information Technology in the Netherlands”, National Report, International Review of Penal Law, vol. 64, pp. 471-506.

committed in an electronic environment such as Internet can be tackled under this Code. The existing characteristics of the crimes which have to be fulfilled according to the law, are applicable to forms of conduct on the Internet.[7]

Researchers have however, also concluded that the application of the defences granted to a printer and publisher under the Criminal Code (based on the freedom of communication) require more in-depth discussion and possibly an amendment to the law. The reason for this being that it is uncertain whether or not links in the electronic communication process can be considered as "publishers" under article 53 of the Dutch Criminal Code. Up to now no case law has been issued that sheds light on the question whether the term 'printing press' may be interpreted independent of the specific communication techniques used.[8] It is proposed that a regulation be formulated that is independent of the present classification of communication techniques.

In this respect the recent proposal of the Dutch legislature to amend article 13 of the Dutch Constitution is important.[9] Under the new article, citizens are guaranteed a constitutional right to the protection of communication. By using the general term 'communication', all new forms of communication will be covered. Surprisingly however, the legislature introduces the possibility that the right may be restricted by law, whereas in the present text of article 13 such restrictions may only be ordered by the court. It is argued that by placing the right to introduce restrictions in the hands of the legislature instead of the court, new forms of communication are in fact outlawed.[10]

The issue of criminal law enforcement is also being extensively debated. We note that traditionally only the persons who reside within the state territory are bound by the law of that state. The possibility of upholding criminal law strongly depends on the territory within which a criminal act has taken place: the *locus delicti.* With the introduction of ICT it has become more difficult, albeit impossible to determine where a criminal offence has taken place. Suppose for instance, a Dutch organization like CP'86 (an

7. Th. de Roos, G. Schuijt, L. Wissink, "Smaad, laster, discriminatie en porno op het Internet", ITeR-reeks no. 3, Samsom 1996, pp. 83-242.

8. In a civil law suit involving the Scientology Church, the court ruled that in principle there is no responsibility for service providers if the provider is not aware of the information content. President of the District Court, The Hague, 12 March 1996 (Scientology/ XS4ALL) Mediaforum 1996/4, p. B59-B61, pp. 61-62; Computerrecht 1996, pp. 73-77.

9. Parliamentary Papers 1996-1997, 25 443, nos. 1-3.

10. See highly critical: N.A.N.M. van Eijk, "(G)een recht op vertrouwelijke communicatie: fax en email vogelvrij", Nederlands Juristenblad nr. 33, 1997, pp. 1554-1555.

extreme right-wing organization) made racially discriminatory remarks through Internet, however these remarks were not transmitted through a Dutch service provider but through a service provider in the USA. To complicate matters further and to escape prosecution, at least in the first instance, the organization did not place the information on the server of the service provider but, for example, from Belgium or Germany. In principle, we may conclude that a criminal offence was committed (under the Dutch Criminal Code: article 137 incitement of hatred – insulting an ethnic group; article 137d – discrimination and violence, and article 137e – publication of discriminatory remarks). However, it is unclear where exactly this offence was committed and whether prosecution can take place. In addition, there is not only the question of whether CP'86 can be prosecuted and penalized but the same question arises regarding the service provider. Similar questions will be encountered with games of chance through Internet (virtual gambling). Whether the jurisdictional rules under the Dutch criminal system offer sufficient possibilities to deal with electronic offences, opinions differ. Whereas no problems can be seen in the previously mentioned 1996 study, others argue that problems occur with respect to established theories about when and by whom sanctions can be imposed.[11]

Finally, it should be mentioned that a study is presently being conducted to make an inventory of and to evaluate the penalization of crimes committed on the electronic superhighway. The principal question to be answered is which developments raise such a threat to the interests of availability, exclusivity and integrity of information, that a criminal law response is appropriate. Also, the study will determine what response, if any, is desired.[12]

2.2 Intellectual Property Legislation

In the 1980s and early 1990s, the copyright questions debated mainly centred around software and database protection. The Dutch legislature has implemented the European Software Directive but has not yet published a draft text containing the provisions for the implementation of the Database

11. See: C.B. van der Net, "Locus delicti op het Internet", Computerrecht, 1996/3; C.B. van der Net, "Smaad, laster, discriminatie en porno op het Internet", Mediaforum 1997-6, pp. 95-96.

12. See: "Inventory and evaluation of the penalization of crimes committed on the electronic superhighway (with the exception of the offences committed through expression)", ITeR studie, project leader Prof. M.S. Groenhuijsen, 1997.

Directive. It is expected that it will not meet the implementation date set in this Directive.[13]

More recently, the prime issues evolve from the fundamental question of whether the traditional copyright concepts, that form the basis of the exploitation rights, can still serve their purpose adequately in an electronic environment. In practice it appears that the strict application of the reproduction right has resulted in a situation in which every reproduction of a copyrighted work is in a technical sense considered to be relevant under copyright law. This is the situation with software and more recently with other copyrighted works used in a digital environment. As a result, almost all types of use of digital copyrighted information are considered to be a restricted act under the copyright law. Various legal experts have criticised this situation.[14] A 1996 study even concluded that it is advisable to abolish the reproduction right as an independent exploitation right under the copyright law. Instead, a broad right of communication to the public should be introduced. The author of the study described such a broad right as 'copyright in (public) access'.[15]

Another recently debated issue is the protection of domain names on the Internet. Who owns 'www.apple.com'? Domain names are chosen to be recognisable, memorable and easily associated with an online company, firm or organisation. Thus, in essence they serve the same purpose as trademarks. Case law in the Netherlands shows that the rights of a trademark may in principle be infringed if an unauthorized person or organisation uses a domain name that resembles this trademark.[16] Case law, however, also shows that an association must be evoked between the trademark and the domain name. For example, if the companies using similar names provide different services this is not likely to constitute an infringement of a trademark. The fact that both companies are involved with Internet does not *per se* constitute any relationship between the services, because Internet is merely a means of communication.[17] Another question which arises is

13. See: P.B. Hugenholz P.B., "De Databankrichtlijn eindelijk aanvaard, een zeer kritisch commentaar", Computerrecht 1996/4, p. 131ff.
14. See: S.J.H. Gijrath, R. van den Hoven van Genderen, H. Wefers Bettink, Intellectueel eigendom in digitaal perspectief, Alphen aan den Rijn/Diegem 1996; P.B. Hugenholtz (ed.), The Future of Copyright in a Digital Environment, The Hague/London/Boston 1996; E.J. Dommering, "Het auteursrecht spoelt weg door het electronisch vergiet. De naderende crisis van het auteursrecht.", Computerrecht 1994/3, pp.109 ff.
15. D.J.G. Visser, Auteursrecht op toegang, 's-Gravenhage 1997.
16. Amsterdam Court of Appeal, April 24, 1997 (Ouders van Nu/Ouders on-line); President of the District Court of Amsterdam, May 15, 1997 (IMG Holland BV/La Bouchere NV).
17. See: Amsterdam Court of Appeal, May 29, 1997 (NTG/Xlink v. xxLINK Internet Services), Computerrecht 1997/4, pp. 170-171.

whether domain names can be fully compared with trademarks, thus using the legal concepts applied to the registration and use of domain names. A problem in this respect is whether the free use possibilities of the trademark system apply to domain names.

Finally, copyright problems should be mentioned which emerge in relation to the development and use of multimedia products.[18] First, problems arise as to how to classify such works under the present copyright system. The reason for this being that multimedia products consist of different types of works (music, text, film, etc.). In certain situations, multimedia products may be classified as databases, meaning that the specific rules laid down in the European Council Directive on database protection will apply once the Dutch legislature has implemented them. Second, in practice it appears highly difficult to trace all copyright holders and negotiate with them on an individual basis to obtain rights of use. To solve this problem it is suggested that electronic collecting societies, so-called ‘one-stop-shops' be introduced.

2.3 Public Information Legislation

For several reasons access to public information is of particular importance. The first reason is that such access is seen as a citizen's or human right needed to ensure the legitimacy of democratic decision-making processes. It is a device in the constitutional system of separation of powers through checks and balances. Its purpose is also to ensure a meaningful and responsible citizenship needed for true democracy. The second reason brings into focus the economic considerations, necessary to develop the information market. The exploitation of official *casu quo* public sector information, under conditions of free and full competition, is needed for the establishment of an information-services market that in its turn is needed to develop information industries. As we enter the information society - a society in which the importance and meaning of information will continue to increase - the issue of access to official information will become increasingly important. Government bodies become aware of ICT's possibilities and become a (co)-partner on the market, in other words the state becomes an *entrepreneur (*it is more gainful for government organizations to sell information). Although in the Netherlands the market for government information is not in full swing at the moment, recent developments indicate that the exploitation of

18. See: P.B. Hugenholtz, “Het auteursrecht, het internet en de informatiesnelweg”, Nederlands Juristenblad 1995/14, pp. 513-519.

government information will experience problems.[19] Problems arise because, on the one hand, the regulations prescribe that government information must be made available to the public at a low cost but, on the other, government institutions should be allowed to sell their information to certain commercial publishers, which excludes others from obtaining the information. The question is what limitations should be drawn up for the future development of the government information market, taking into account not only the guaranteed constitutional principle of public access to information, but also its position as an equal competitor on the market. Increasing social inequality could result from the commercialization of government information (info-rich/info-poor).[20] Unlike Sweden, the Netherlands has not yet established a national electronic register of public sector information. Thus, the lack of information on where and how to find this information appears a major barrier. It is further mentioned that in the Netherlands the synergy between the private and the public sectors often results in privileged positions for certain companies. The recently privatized companies, in particular occupy a favourable position because they are often still in some way connected to the public sector. Also, the cooperation between the two sectors appears subject to specific conditions. Finally, problems arise in relation to the applicable rules. The Netherlands has a Public Access Act. However, in view of the above developments experts argue that the existing regulations on access have to be reassessed, and possibly adjusted to a new type of society.[21] Recent developments show that the first steps towards such a reassessment have indeed been taken. In early June 1997, the Dutch Council of Ministers adopted the working document "Towards accessibility of public sector information".[22] The document contains various plans for the commercialisation of this information, thus aiming to give a strong impulse to

19. See: S. van der Hof, "Overheidsinformatie in de etalage", ITeR-reeks no. 5, Samsom 1997, pp. 3-162; A.A.L. Beers, Informatica Publica: publieke toegankelijkheid van electronische overheids- informatie, Den Haag: Rathenau Institute 1996, Study 34; Rathenau Institute, Elektronische toegankelijkheid van overheidsinformatie, Amsterdam: Cramwinckel 1996, R16; Rathenau Institute, Toeval of noodzaak? Geschiedenis van de overheidsbemoeienis met de informatievoorziening, Amsterdam 1995.

20. The amount of information produced by the government is so overwhelming that (effective) access to this information is only possible by using an index or search system. Because this system is expensive access is, especially for those who are financially less well off, effectively barred.

21. See: A.A.L. Beers, Informatica Publica: publieke toegankelijkheid van electronische overheids- informatie, Den Haag: Rathenau Institute 1996, Study 34; A.A.L. Beers, "Overheidsinformatie op Internet", Nederlands Juristenblad 1996/41, pp. 1708-1716.

22. The document was sent to Parliament on June 10, 1997 (Parliamentary Papers 1996-1997, 20 644, no. 30).

electronically distributed public information. Also, government organisations are to electronically provide information on their activities, documents, etc., so that they become more transparent for citizens, who subsequently may become more involved in the democratic processes.

2.4 Personal Data Protection

In contrast to access legislation, which seeks to provide access, data protection legislation is primarily protective in that in principle it tries to reduce the availability of information on persons.[23] However, neither data protection legislation nor access legislation can provide unrestricted protection or unrestrictive access. Personal data can sometimes be disclosed to other parties because of overriding interests. The European Union has addressed the issue of personal data protection in a Directive, which is presently being implemented in the legal system of the Netherlands (*Data Protection Act*).[24] With the rules on personal data protection being implemented and applied, new problems of legislative interpretation may be expected to arise. Besides the general (interpretation) questions that arise as a result of the European Directive, the Dutch privacy discussion focuses on the following more specific issues.

The emergence of new technologies results in a tendency towards an expansion of the concept of privacy. The line of division between personal data and anonymous data or object data is becoming less relevant, for example in case of profiles of target groups. Principally the possibilities which new information and communication technology provide to convert specific data to personal data can create new problems. Methods of reidentification can be: response knowledge, coupling or databank comparison and spontaneous identification. Response identification occurs for example, when someone learns from an anonymous file whether a certain individual has participated in a survey. Through coupling or comparing files, two or more data files can, with computerized help, be compared with each other resulting in the identification of the individual. Spontaneous identification is possible when an individual is considered to be ‘unique' in a certain aspect, such as Her Majesty the Queen or the Minister of Justice. This can sometimes be avoided by carrying out certain technical measures to ensure

23. See: J.E.J. Prins et al., “In het licht van de wet persoonsregistraties: zon, maan of ster?”, ITeR-reeks no. 1, Samsom 1995; G. Overkleeft-Verburg and H.H. Vries, “De Wet persoonsregistraties. Norm, toepassing en evaluatie”, Themis 1997/6, pp. 259-260.

24. See: J.M.A. Berkvens and J.E.J. Prins, “De bescherming van persoonsgegevens: van WPR naar WBP”, Recht en computer, Deventer 1997, pp. 315-369.

that data cannot be traced to individuals and that the appropriate legal rules are applied. In addition to the possibility of reidentifying anonymous data, an individual's object data can also be traced. An example of ‘object data' is the data which is registered, within the framework of the National Car Licence Card, or information regarding the sales price of houses as in the case of a unique building where it is possible to determine the identity of the owner by consulting the land registry. Thus the question arises whether object data should also be brought within the ambit of personal data protection.[25]

ICT is economically valuable but from a privacy point of view, its development also hides a threat and that is the possibility of manipulating data. The expansion of data analysis methods such as knowledge discovery in databases (also referred to as data mining) has also far-reaching consequences for privacy and the privacy concept. These methods stimulate for instance, the birth of so-called data-warehouses (specializing in and geared to large and widely oriented data collection) which can act as a basis for building a profile. Tolerance of these data-warehouses must be questioned if they can be used for all kinds of means and ends. To date, the use of profiles has started to receive attention in Dutch privacy literature.[26]

It is to be expected that after the implementation of the European Directive in the Dutch legal systems, prime attention should be given to the questions that arise in relation to the above situations and technologies.[27]

2.5 Consumer Protection Legislation

The development of commercial activities on the Internet is strongly promoted both at a national and at European level and now raises new questions as to the protection of consumers who purchase goods and services by means of electronic ordering (so-called ‘electronic consumers'). The most striking features of electronic transactions are first, that they are cross-border transactions and therefore challenge the traditional concepts as to which law is applicable, and second, that brand new services are offered to consumers.

Traditional questions must therefore be answered from different perspectives, not only because transactions are now cross-border activities but also because the very infrastructure of the market is accompanied by specific legal

25. J. Holvast, “Persoonsgegevens of niet: dat is de vraag”, ITeR-reeks no. 2, 1996.
26. H.J.M. Gardeniers, R.W. van Kralingen and E. Schreuders (1996). Knowledge discovery in databases; privacyaspecten van informatiemijnbouw. In: Privacy in het informatietijdperk, pp. 69-84. Voermans en Nouwt (eds.) SDU, Den Haag.
27. See: P.J.M. Kolkman, ”Digitaal bekeken”, http://cwis.kub.nl/~frw/schrdijk/cri/kolkman/mjmib9.htm.

problems. In the Netherlands considerable attention is being paid to the question of whether the fundamentals of consumer law can be applied as such, considering the new aspects of commerce. Two issues are at stake: the consumer himself has to be granted satisfactory protection or else there is a risk that he is deterred from purchasing on the network through distrust. This is a condition for the successful development of commercial activities. Another requirement for a proper development is the removal of national discrepancies in consumer protection laws. Specific legal problems regarding (consumer) protection are to be considered from that perspective: privacy protection, liability and redress, evidence, electronic signature, payments, security, formation of contracts (offer and acceptance), etc.

In 1996, the Dutch Ministry of Economic Affairs asked the Social and Economic Council (*SER*) to advise the Ministry on consumer issues in relation to new markets, such as the markets of biotechnology and information technology. The *SER* reported by means of its Commission for Consumer Affairs.[28] In the report, the Commission noted that in-depth studies are necessary in order to determine whether legislative action is required to protect consumers who buy goods or services by means of electronic mechanisms such as Internet. Also, the report stressed that the Dutch legislature should focus its attention more towards the European dimension of the legal problems surrounding electronic consuming. Finally, attention was drawn to the possibilities of the mechanism of self-regulation (codes of conduct).

A sub-commission of the aforementioned Commission for Consumer Affairs is currently studying the relevant legal issues that arise in relation to electronic consuming.

2.6 Some General Legal Concepts

ICT has had a dematerializing effect on many processes. Hand-written documents are, for example, being replaced by electronically produced documents, information is no longer provided in writing but delivered electronically and software is no longer presented on a disk but downloaded via the network. Examples in the Netherlands of such changes are the Sagitta-project (an electronic document system used for customs purposes) and the possibility to file tax returns by means of an electronic system. Further, computers maintain an inventory and proceed to re-order a certain product automatically once the relevant minimum stock has been reached. In

28. Commissie voor Consumentenaangelegenheden, “De consument op nieuwe markten”, SER, February 7, 1997/31.

view of the fact that in our legal system a declaration of will and the justified trust of the individual are central principles as a condition for a legal action, it is intriguing to challenge the issue of whether legal actions can be instigated through the use of EDI techniques.[29]

Also, because we have a legal system that is very often based on physical objects, it is necessary to explore whether ICT developments demand revision of the legal concept of 'document'. In many cases the law demands procedural requisites. Written material such as consignment notes and wills must comply with certain procedural requisites in order to be considered valid. If these documents were to be replaced by electronic versions, this could mean that, in the event of unchanged procedural requisites being demanded, an electronic version would be absolutely worthless. As it is the present tendency to, for example, send consignment notes electronically, steps must now be taken to avoid any unintended effects.

In the Netherlands recent attention has primarily focussed on the legal status of digital signatures and digital documents.

The functionalities of a digital signature mainly equal those of a manual signature; the digital signature realises an association between a person (position or organisation), and the signature as a result of which a (legal) intention is expressed. The aforementioned at the same time indicates the weakness of the digital signature, for the digital signature is often not of a personal nature like the manual version and therefore it does not ensure the determination of a unique identity (a prerequisite for *e.g.*, notarial deeds). However, a digital signature can, contrary to a manual signature, offer protection against, for instance, forgery and it can guarantee confidentiality of messages. Various studies and developments in the Netherlands show that Trusted Third Parties[30] can play an important part in the latter, by enforcing the observation of the necessary safeguards for authenticity and integrity by means of rigorous key management.

Like in many other European countries, the digital signature is in the Netherlands subject to legal insecurity. Dutch case law shows only very few examples of court decisions which equate certain electronic documents and digital signatures with their written equivalents. The decisions, however,

29. The question whether a contract can be made by a computer is the topic of a research project (see: F.A.M. Klaauw-Koops, "Totstandkoming van een overeenkomst via EDI", Recht en EDI, Deventer 1994, pp. 35-52.)

30. See: H. Franken and A.M.Ch. Kemna, "Bewijs, bewaring en geschillenbeslechting", Recht en Computer, Deventer 1997, pp. 230-270; R.E. van Esch, "Elektronische rechtshandelingen", De notaris en het elektronisch rechtsverkeer, 's-Gravenhage 1996; H. Franken, "De notaris als Trusted Third Party", De notaris en het elektronisch rechtsverkeer, 's-Gravenhage 1996; S. van der Hof, "De juridische status van de digitale handtekening", ITeR-reeks no. 7, 1997, pp. 3-67.

relate to procedural law and do not shed light on the impact of digital signatures and documents on civil law in general, nor on the statutory provisions on legal acts in particular. An example of the above-mentioned case law is the decision of the Dutch Supreme Court, in which it held that a faxed writ is valid, despite the fact that the law merely refers to a signed and written writ.[31]

It should be mentioned at this point that in the Netherlands, parties may and very often will determine the legal status with respect to, for instance, electronic evidence in order to interpret the voids and obscurities which occur. Parties are permitted to regulate the value of evidence through a private-law instrument. Perhaps due to this, the Dutch legislature has not yet considered legislation in the field of digital signatures.[32] Also, in legal literature objections have been raised to the general and unconditional legal recognition of digital documents and signatures on a par with their written equivalent. A recent study thus suggested not to amend and adapt existing legislation or to draft new legislation. For the time being, self-regulation appears in most situations to be a good solution. Only in situations where certain legal matters remain shrouded in uncertainty and cause problems in day-to-day practice, can new legislation be considered. In other situations one has to rely on case law.[33]

In light of the discussions on the legal status of digital signatures and electronic documents, mention should be made of the 1996 report of the *Koninklijke Notariële Broederschap* (Dutch Association of Notaries), that centred around the possibilities of the use of ICT in the notary practice. One of the questions considered was whether the traditional notarial deed could be replaced by a digital variant. There are two important aspects involving the legal value of a notarial deed: i) the validity of the notary agreement and ii) the notary's own observations and tasks.[34]

Re i) In principle, the signature on a notarial deed could be replaced by a digital one. The notary furnishes an electronic act with an electronic signature. However, the problem which arises here is that it cannot be completely verified whether the addition of the electronic signature was in

31. Netherlands Supreme Court 4 June 1991, Netherlands Supreme Court 1991, 791. See also: Netherlands Supreme Court 27 November 1992, Nederlands Juristenblad 1993, 569.
32. See on the present position of the Dutch legislature: S. van der Hof, "De juridische status van de digitale handtekening", ITeR-series no. 7, 1997, pp. 32-36.
33. S. Huydecoper, R.E. van Esch, "Geschriften en handtekeningen: een achterhaald concept?", ITeR-series no. 7, 1997, pp. 69-325.
34. By signing the notarial deed, the notary guarantees the identity of the persons appearing before him and thereby the authenticity of their signatures. This guarantee is not only binding between the involved parties but also as regards any third parties.

fact that of the notary who signed the document. Nor can it be ascertained whether the declaration by the notary in his official capacity was carried out. Since, for all purposes it is not certain that the notary had in fact ascertained whether the relevant parties were those they purported to be during the signing of the act. It could be that the junior notary had signed the electronic act provisionally.[35]

Re ii) The condition that the absolute evidentiary value of the notarial deed is restricted to the notary's own observations and authorization as a notary can, because of the introduction of a functional electronic equivalent of the notarial deed give rise to several problems. The fact is that an electronic environment can restrict the possibilities of a notary being able to carry out his/her own observations. The notary must in the case of execution of acts which contain final wills and testaments and require witnesses, ensure that the witness understands the contents of the act. A notary will no longer be able to perform this duty if witnesses submit their declaration electronically. Although there are several safeguard techniques (such as the encryption of messages and digital signatures) which can guarantee that the contents of a declaration of parties has not been altered during transmission on the network, the problem still remains that the circumstances under which the parties submitted their declarations cannot be validated by the notary through an electronic medium. These were not made in his/her physical presence. The extension of the guarantee is, from this point of view, limited to the observations of the notary which depend upon the way in which the electronic statement was received.

The notarial deed is therefore an example of the fact that out-dated concepts (written notarial deed) are no longer valid, while, at the same time new concepts (for the time being) cannot replace the essential value and rationale of the traditional notarial deed. It was concluded that from a legal evidence point of view, the electronic version of the notarial deed cannot be compared with the notarial deed as we know it. Sole identification cannot, as yet, be guaranteed.

35. In the Netherlands the ruling theory is however, that a junior notary is not authorized to undertake acts in the name of the substituted notary. Whoever contests the authenticity of the act must produce evidence that the signed agreement is not true and legal.

2.7 Tax Legislation

The fact that information is not presented in written form but electronically also creates problems in other areas of law. When submitting written information it is considered that this is a commodity (*e.g.* a book), when electronic information is submitted it is considered a service. This distinction is, for example, important for applicable law. Several years ago, this distinction was especially critical in relation to product liability for software. More recently, the Dutch discussion in this light has focussed in particular on taxation problems.[36] The following issues were addressed:

First, it is noted that the present system for levying tax is based on the existence of states and geographical boundaries. For example, income tax and turnover tax are levied in respectively the country in which the income was earned and the country in which the goods were sold. ICT has important consequences for the possibilities and impossibilities of levying tax.Transactions which are carried out via computer networks are difficult to trace and happen so quickly that the tax authorities have little control over these transactions. In addition, territorial boundaries between states disappear in the maze of transactions within the network. As soon as cross-border transactions are carried out, then conflicts can arise regarding who should levy the authorized tax. Each state which is involved in (profits of) a transaction can, in principle, stake its claim to levy tax. This leads to questions such as: where should the earned income or profit be taxed and where should the turnover tax be levied? It would appear that through the introduction of ICT, fiscal sovereignty could seriously be affected.

These problems become clearer where a levy on tax for delivered goods or services provided is concerned. The arrival of electronic transactions makes it difficult to tell the difference between goods and services. For example, can in some cases the delivery of data in the fiscal-technical sense, be considered the same as the delivery of goods or does this always refer to services? The distinction is very important for turnover tax purposes. In principle, turnover tax on goods is levied from their place of dispatch at that moment. In the case of turnover tax on services this is levied in the place of residence of the service provider. In both cases profit and income tax are levied on respectively the place where the deliverer of goods or provider of services lodges or resides. If a company also has a permanent address or place of residence abroad, then part of the profit from income can also be allocated to another fiscal territory.

36. See: H.H.M. Maathuis, “Cybertax: the End of Tax Assessment”, Emerging Electronics Highways; New Challenges for Politics and Law, The Hague 1996; B.G. Zadelhoff, Of de BTW het redt met telecom en Internet, Deventer 1996.

In the event of furnishing goods and providing services, the rules regarding tax levies are also based on the physical location where the goods are held at the time of delivery or from the address where the services have been rendered. When dealing with transactions via computer networks there are problems because physical locations and frontiers no longer play an (important) role. To illustrate: providing access to general data through an on-line database can be regarded as providing services. The value of the service is reflected in the way the data are organized and access is made possible. If the provider of the services controls database servers at a distance in different countries, one can query where the services originate from. In the country where the provider maintains the database, in the country where the database service is physically located or from the country where the user of the services resides?

A similar problem arises as a result of the provision of so-called shareware. This is software which an user can download usually from a large number of different locations. As soon as the evaluation period has elapsed, the user must register and pay for the use of the software. Upon payment the user becomes, for tax purposes, the economic owner of the software and the transfer of software is, for tax purposes, registered as the delivery of non-physical goods. In such cases, the question is "where were the goods at the time of delivery"? At one of the many service providers of software, on a server, or in the country where the company which developed the software is located or operates from and where payment is finally made to? Furthermore, there is also the question of royalties and taxation in the country from which payment is made.

In view of the fact that tax authorities decide independently from one another whether tax should be levied, a difference in interpretation can arise between the different states. It can happen that a certain state regards a server managed from abroad as a company with a permanent residence or abode within the borders of that state and therefore determines that the company falls within the fiscal territory or under that location, whereas another state can decide the opposite. Because of this difference in interpretation it can occur that either double or indeed no tax is levied which, from an economic perspective, can have significant consequences.

2.8 Evidential legislation

In many situations, the issue of the value of electronic evidence is dealt with in a contract.[37] As mentioned earlier, in the Netherlands parties are permitted to regulate the value of evidence through a private-law instrument. This is in contrast to certain other European countries. Nevertheless, from different studies undertaken it becomes clear that with paperless communication the absence of traditional methods of proof requires that new methods should be introduced to secure the value of such evidence before the court.[38] Issues such as authenticity, identification, integrity, and reliability are of prime importance at this point. Could standardisation and certification be of relevance? What about the value of cryptographic techniques and what will be the consequence if certain governments (as the Dutch in the past) intend to prohibit the use of crypto techniques in the light of fighting organised crime? Also the position of Trusted Third Parties (TTP) should be further studied in the light of the value of electronic proof.

Although cryptography may be considered scientifically secure, it cannot be said that it can be regarded as compelling evidence in court. The use of a digital signature as evidence will depend on other factors as well. A signature key can, in principle, and in many implementations (Rivest Shamis Adleman, Pretty Good Privacy), also be used for encryption for confidentiality purposes. Given the disparity between these two functions, users should be encouraged to use separate key pairs, and to keep a separate private key for signatures only. However, in current practice, many people use a single key for signing and encrypting. If this key is escrowed (for recovery purposes or for legal investigation purposes), the evidential value of a signature will be weakened, as the key is not the exclusive property of the (supposed) signer. Therefore, key escrow will have to be taken into account. Further, contrary to paper signatures, a digital signature is in principle transferable: another person can make the signature for someone else. Procedures will have to address this issue, if a digital signature is to have evidential value in court, with implications for contracts, non-repudiation and burden-of-proof.

Finally it is mentioned in Dutch legal literature that in general, there is a discrepancy between legal culture and science. Although technical evidence is gaining in importance, conservative judges may be wary to allow a

37. In the Netherlands, the admissibility of electronic proof is not a problem due to the fact that the Dutch Code of Civil Procedure works with a system that allows all types of evidence.

38. See: J.E.J. Prins, “Bewijsaspecten rondom EDI”, Recht en EDI, Deventer 1993, pp. 95-114; H. Franken and A.M.Ch. Kemna, “Bewijs, bewaring en geschillenbeslechting”, Recht en computer, Deventer 1997, pp. 230-270.

technical application (the working of which must be incomprehensible to them) to replace such an important feature as the signature. Education and technical assistance in courts may be called for to address this issue. The role of expert witnesses needs to be clarified.

Thus, one could conclude that the issues raised in relation to electronic evidence concentrate mainly on the mechanisms that may provide such evidence with the same value as traditional written proof.

2.9 Liability Issues

Ever since the introduction of information and communication technologies, liability is an issue for deliberation and court rulings. In the 1980s, attention was focussed on the liability of software advisors and software product liability questions.[39]

More recently, it is the liability for and control of information distribution that has been the subject of recent court cases. As mentioned above, the Scientology Church has attempted to hold an Internet access provider liable for the contents of the webpage of one of its subscribers.[40] However, Internet providers are not the only ones confronted with these issues. For various situations, traditional concepts such as blame, negligence, damages, fault, etc. have to be re-evaluated in the context of electronic networks. The same holds for control of information content; when can a provider be said to have actual control of information content? Since these subjects are 'on the move' it is difficult to predict exactly how concepts will crystallise in their new form. In the case of the Internet provider there seems, however, to be a tendency towards limited liability of the provider.

Also, the liability of TTPs (notably certification authorities) for damages related to digital signatures and public-key certificates is *terra incognita*. Many policy documents recognize the importance of addressing liability, but few have analysed the particular circumstances under which TTPs can be held liable for particular damages resulting from particular breaches of security.

39. See: R.J.J. Westendijk, Produktaansprakelijkheid voor software, 1995.

40. See footnote 6.

3 Applications and their legal problems

3.1 Smartcard (Payment) Applications

With the introduction of a smartcard with a multi-functional application (*e.g.* a health-care application in combination with a payment function and public transportation ticket), we see that for the first time a large amount of differentiated information can be assembled and made available. This heralds important legal consequences that are being discussed in Dutch legal literature. Who is the ‘owner' of this multi-functional smartcard on which several application providers have placed valuable information concerning their companies' activities?[41]

As regards the payment function of a smartcard, there is major competition in the Netherlands between two major initiatives for a prepaid card (the *chipper* project and the *chipknip* project). Both systems use separate general conditions. The question of whether electronic money should be treated as money is debated.[42] In the meantime, the Dutch Central Bank (DNB) has formulated a set of minimum requirements that should be taken into account by the issuing banks. The requirements concern: the general characteristics of the scheme, the institutional and organisational setup, the legal aspects, the issuing, the accounting and administrative procedures, float management, security, technical and infrastructural features. Each of the afore-mentioned requirements has been specified in detail.[43] The DNB has the power to supervise the new electronic money initiative of the smartcard because the issuers of this card need a banking licence due to the fact that such prepaid cards are qualified under the Banking Supervisory Act as equivalent to deposit taking.

41. Not only is this issue being discussed in Dutch literature, but also the position of ‘owners’ of numbers, e-mail addresses and their Internet equivalents are the subject of discussion (compare the problems concerning number portability).

42. See: R.E. van Esch, “De chipknip: het virtuele chartale geld”, Computerrecht 1996/4, pp. 126-130; R.E. de Rooij, “De chipknip: een juridische verkenning”, Nederlands Juristenblad 1996/14, p. 511; J.M.A. Berkvens, “Juridische status van de chipknip-betaling”, Bb 1996/2, pp. 13-14.

43. More in detail: H. van der Wielen, “Electronic Money: a European Perspective”, speech given on February 4, 1997 at the seminar “Electronic Money” hosted by the Bank of England.

3.2 Encryption

The arrival of ICT has made it possible to communicate with each other on a large scale through electronic communication media. These technological developments also mean that our traditional methods of protecting data no longer suffice, but it goes without saying that our need to protect valuable data has not diminished. To solve this problem advanced mathematical techniques have been developed in the form of encryption.

The reason why encryption is chosen is not only to keep data secret but to guarantee the integrity of data and protection of privacy. In an environment where business orders are electronically processed and sent, data integrity is essential. Secrecy plays an important role when transmitting company details or making designs in a virtual environment such as, for example, new cars. Also, privacy is a key issue when transmitting medical data electronically. However, as in many cases, new techniques will not only be applied for good purposes but also for bad ones. We are now being warned about criminals who can no longer be 'tapped' effectively. This has led to the view that encryption should be prohibited or at least strictly controlled.[44]

In the Netherlands the question as to whether and how to regulate encryption has been highly debated, in particular when in 1994 the Dutch legislature contemplated the introduction of legislation.[45] The proposed rules were severely criticized. In the discussion, experts dealt with the conflict between the right of personal data protection and confidentiality versus the investigation interests of the public authorities. Also, the powers to be attributed to key centres formed a point of discussion. After it became clear that both control and enforcement would be major obstacles to effective legislation, the proposed rules were abandoned. At present some legislative initiative is considered necessary, but only worthwhile taking if it is done in line with the developments at an international level. Thus, the Dutch legislature awaits a more favourable (international) climate. In the meantime, no legislative rule forbids the use of cryptographic techniques in the

44. More detailed: F.P.E. Wiemans, J.M. Smits, H.C.A. van Tilborg, "Encryptie – justitiële en particuliere belangen, een verkennende beschouwing", Delikt en Delinkwent 1994/4, pp. 340-359; A.M. Kemna, A. Tuinder, "Regulering van encryptie", ITeR-reeks no. 3, pp. 3-80; E. Verheul, B-J. Koops and H. van Tilborg, "Public Key Infrastructure", Computer Law and Security Report, Elsevier Science Ltd. 1997, pp. 3-14.

45. Voorontwerp van wet inzake cryptografie, Mediaforum 1994/6, p. B49; R. van den Hoven van Genderen, "Het voorlopig voorontwerp tot verbod van cryptografie. De horror vacui van de ondoorbreekbare beveiliging", Computerrecht 1994/4, pp. 157-162; A. Patijn "Crypto: een zege of een bedreiging?", Computerrecht 1994/4, pp. 144-149.

Netherlands but telecommunication legislation requires telecom operators to offer the possibility to decrypt communication when required.

3.3 Trusted Third Party (TTP)

Encryption is closely related to the instrument of the so-called trusted third party (TTP). Lately, the position and possible tasks of this type of independent third party has received considerable attention in the Netherlands. Being an independent third party, a TTP can guarantee the confidentiality, integrity and authenticity of messages sent by means of certifying a public key with the use of an asymmetric cryptosystem (also called public key cryptosystem). The TTP fulfills the role of a certification authority.

It is believed that the instrument of an independent (trusted) third party will play an ever-increasing and greater role in the information society (not only for the above-mentioned functions such as the time stamping of documents and signatures, the filing of and possible issue of certain information, escrow,[46] the provision of electronic evidence). There is a growing demand in the Netherlands for these new kinds of services which of course, also generate legal issues. For example, if the TTPs are to adequately fulfil their necessary role, the liability for and qualification of such services requires that the position of TTPs is specified and made clear in the law, such as the telecommunication rules. Furthermore, guarantees must be given regarding the reliability of TTPs (for example through a certificate issued by a super or top-level TTP).

At present, commercial organisations are taking some first tentative steps towards developing and offering TTP services on a commercial basis. The Ministry of Economic Affairs together with the Ministry of Transport & Public Works have announced the development of a set of conditions that organitions have to comply with when operating a TTP.[47] In the meantime, various (academic) research projects specifically deal with the legal implications of the TTP instrument.

46. An escrow construction is one by which a third party (e.g. a TTP or notary) keeps information to safely ensure the relationship of the two as agreed. Such security can be important in, e.g., bankruptcy of a software producer or in cases of contractual disputes.

47. Netherlands Government Gazette, March 18, 1997, p. 54.

4 The characteristics of on-line communication

In order to adequately assess the legal implications some of which have been described above regarding the use of ICT and more specifically Internet, we need to consider in what way ICT processes influence our day-to-day actions and have implications for the legal description of these acts. By looking at the legal consequences of informatization at a meta-level, *i.e.* from the perspective of characteristics and processes and thus clustering these consequences, a clearer understanding could be gained as to what the impact on our legal system is really about. Several more recent studies by Dutch legal experts have focussed on the characteristics of ICT that have an impact on the law, instead of discussing the issues on a topic-by-topic basis.[48]

In comparison with traditional (paper-based or oral) communications, on-line communication works with different concepts. Firstly, in a digitized and interconnected environment, communication results in indeterminacy regarding the scope of possible relations between individuals and organizations. The dynamics of on-line communication allow people to make and send an infinite number of identical copies with a simple keystroke and thus deliver messages simultaneously to many other people and entities. For this reason, communication is no longer an overall person-to-person (unique) issue. This necessitates for example different approach to the traditional paper-based functions of originality and uniqueness.

Secondly, electronic communications move from point-to-point applications to open and often highly decentralized communications. As a result, in the Internet environment, it is almost impossible to track the use of certain documents and thus, for example, to uphold relevant intellectual property rights.

Thirdly, with the increasing cross-border scope of networks, computer systems in other countries may be used as easily as they may be used in the users' home countries. Distance becomes irrelevant. In addition, as a result of the use of so-called self-routing systems, the route actually taken by an electronic message becomes an issue depending on the amount of electronic traffic, *i.e.* it is determined by chance. It is becoming increasingly difficult and sometimes impossible to find out by means of which systems – located in which country – a message was transmitted. From a legal perspective,

48. For more details see: J.E.J. Prins, R.W. van Kralingen, "De invloed van ICT op het recht", Volatilisering in de economie, WRR (Dutch Scientifc Council for Government Policy) Studie V 98, The Hague 1997, pp. 105-123; E.J. Dommering, "Internet: een juridische plaatsbepaling van een nieuw communicatieproces", Volatilisering in de economie, WRR (Dutch Scientifc Council for Government Policy) Studie V 98, The Hague 1997, pp. 129-150.

there may thus not be a straightforward answer to the question of which of the jurisdictions the message passed through may claim authority and what national law is thus applicable.

Fourthly, compared to the ‘slow’ traditional means of communication, electronic interaction is a highly dynamic and real-time process, allowing people even to interact immediately. Besides the pros of this development, there are also the cons. With distance selling, *e.g.*, the speed of presentation and communication results in a virtual shopping mall where consumers are given neither the opportunity nor even the time to grasp all (legal) implications. E-commerce therefore erodes the attributes that are inherent in ‘slow' communication.

The above four characteristics of electronic communication result in the following processes:

* fading geographical boundaries: electronic information defies geographical boundaries. Computer systems abroad can be as easily consulted as a system in one's own country;
* fading organizational boundaries (virtualization): information and communication technology (ICT) increases the opportunities of creating, according to the circumstances at a given time, the right organizational mix. As a result, inflexible ‘physical' organizations will increasingly be replaced by dynamic ‘virtual' organizations;
* changing social relationships: in comparison with traditional media, ICT offers new horizons for interaction between sender and receiver. In fact, ICT offers the participants of economic traffic new participation possibilities (for example between producer and consumer or between the public and private sectors);
* concentration of information: ICT offers many opportunities for the optimization of the information chain. The possibility of observation, retention, transmission and adaptation of information is ever-increasing and the implications of this are very clear: it enables an enormous quantity of information to be used systematically, reliably, quickly, cheaply and inconspicuously;
* dematerialization: hand-written documents are being replaced by electronically produced documents, information is no longer provided in writing but delivered electronically and software is no longer presented on a disk but downloaded via the network;
* reduction of human involvement: physical contact between people will increasingly be replaced by electronic contact. Also the introduction of ICT applications has very often made human involvement unnecessary (a supplies management system can order products automatically when the supply figures indicate that a minimum is in store);

* changes in speed and deadlines: with ICT, processes are no longer thought of in terms of man-hours and physical distance.[49]

5 Suggestions for a regulatory policy

As mentioned in the introduction of this report, the Netherlands has initiated a National Action Plan for the Information Highway, the purpose of which is to stimulate the use of the Internet. Such stimulation encompasses among other things the removal of legal barriers. This aim is being realised by means of the so-called National Programme for Information Technology and Law *ITeR*, established in March 1994. By means of this programme, the Netherlands Organisation for Scientific Research *NWO* in cooperation with five Dutch ministries[50] aims to stimulate and coordinate the research in the area of law and information technology. For this purpose *ITeR* has since 1995 funded various projects in four selected areas: 1) the legal status of information and developments in supplying information, 2) the availability and exclusivity of information, 3) telecommunications infrastructure, 4) IT in legal and public administrative organisations. The results of the different projects are published in a series of books: the *ITeR* series.[51] The *ITeR* programme officially ends in 1998, but it will take longer before all projects are concluded.

In general, one could describe the present approach of the Dutch legislature with respect to ICT developments as one of 'sit and wait'. This could be a reaction to the considerable criticism that has been expressed in the past concerning information technology regulation. This criticism can be viewed in different ways such as complaints about too much control, complaints about the complexity and range of regulation towards companies, organizations and citizens, complaints about the impossibility of controlling the regulations and the lack of legitimacy of the law. In 1996, the Ministry of Justice launched an ambitious project to consider the various problems and interests at stake from – what can be called – a meta-level point of view. The project – entitled "Uitgangspunten van wetgeving op de elektronische

49. For more details see: J.E.J. Prins, R.W. Kralingen, "To Regulate or Not to Regulate: Prevalence and Impact in a Virtual Society", The EDI Law Review, no. 2 1997.

50. The Ministry of Economic Affairs, the Ministry of Home Affairs, the Ministry of Justice, the Ministry of Education, Science and Cultural Affairs and the Ministry of Transport and Public Works.

51. Published by Samsom Bedrijfsinformatie, Alphen aan de Rijn. All books have English summaries of the studies. For more information on the programme: ITeR@nwo.nl

snelweg" – aims to determine the criteria on the basis of which the legislature should decide whether or not it is useful to undertake regulatory action. It is scheduled to deliver a working document to the Council of Ministers by the end of 1997.

In the meantime, various other governmental and non-governmental organisations have also launched projects that deal with 'law and ICT' in one way or another. Mention has already been made of the activities of the Social and Economic Council in the area of consumer protection. The Dutch Scientifc Council for Government Policy in 1996 launched a project called "Volatilisering in de economie" which includes law-related issues of ICT.

All afore-mentioned projects (are expected to) show that in order to assess the required type of regulatory action, a more juridical-strategic insight into the use of ICT is considered necessary, an insight which goes beyond mere facets of regulation. Various experts in the Netherlands thus argue that steps towards an integrated – mainly technically independent – type of regulation should be made. The above-mentioned insights of which ICT characteristics have an impact on the law and the legal concepts used, can be considered the first tentative steps towards a better understanding of how to approach ICT regulatory action. What is already becoming clear is that legal experts as well as policy makers question whether constraints should always be removed through harmonization of laws. ICT offers such a large and ever-expanding range of possibilities that it is impossible to regulate all its facets. In the Netherlands the following general considerations as regards regulatory action are discussed.

5.1 Convergence and Divergence

ICT brings about a dualism in the character of the regulatory instruments. On the one hand we observe that a convergence of law and regulations is necessary. Experts point in this respect to the distinction between broadcasting and telecommunication that is no longer useful, and the necessary integration of copyright regulations concerning pictures, text and sound. It is important that such closely related territories are not approached from different angles. The first regulation tendency is therefore convergence which demands in addition not only a European but a world-wide approach.

On the other hand, there will be a greater demand for diversity of norms. It is almost certain that a division must be made between the production of information and its transmission. Also, an increasing specialization of regulations is necessary in light of the fact that the information society will be increasingly characterized by strong differences in sectors, processes and

activities. This means that different norms and values will be applicable for different cases and at different times. For example, with privacy matters, the implementation of digital medical technologies cannot be compared with the use of intelligent software for a direct-marketing policy.[52] Although at a technological level, ICT developments are comparable, the results of these developments within specific contexts and within certain relationships and relevant interests are highly different.

5.2 Co-production

It can be queried whether summarized and clear regulations can be created, especially where divergence of regulations is required. The question which then arises is how should the necessary dual regulations be made effective? It is proposed that within an informational society there is a greater need for rules which standardize and make things more flexible than a framework of laws that dictates and thus immobilizes.

First and foremost it must be stated that the regulation of certain developments in a society can be pursued and accomplished in more ways than by laws and regulations. Law and regulations in various situations are not necessarily the best type of policy intervention.The present ICT developments show that the increasing diversity and variety of information processes cannot be approached by a universal regime. At the legislative level this implies that merely generalized norms and guarantees should be set, requiring different social sectors to regulate the situations in more detail (self-regulation), for example by means of a code of practice. As a result of this approach the role of the legislature shifts somewhat but remains important. This approach is often called co-production. By relying on the – flexible – opportunities of self-regulation, it can be avoided that legislation has to utilize too many technologically dependent norms. The call for more technology independent norms is closely related to the call for (flexible) context-bound norms and policy instrumentation.

52. Compare the findings of the evaluation of the Dutch Data Protection Act: J.E.J. Prins, Zon, Maan of Ster. In het licht van de Wet persoonsregistraties, Alphen a/d Rijn 1995.

5.3 Technology instead of Legislation

Various reports in the Netherlands mention a third steering possibility besides legislation and self-regulation.[53] Technological innovations can be seen as important opportunities for the effective implementation of legal regulations. To a certain extent the use of some technical facilities may even make legislation on certain developments no longer necessary. One can think in this respect of the terrain of maintaining intellectual ownership (digital watermark) and privacy (insertion control, integrity-checking, auditing and admission control). Attention can also be paid to the possibility of reloadable chipcards which can be used for anonymous services. On the one hand this means a relief from (financial) tasks for companies and, on the other, a more effective protection of the consumer's privacy.

6 Conclusions

The dynamics of society increase as a result of the implementation of ICT. Connections become weaker, changes take place quicker and innovations appear one after another. Traditionally the law is not an instrument which can be applied for the regulation of dynamic processes and rapid (technological) changes. The concept of a ‘malleable society' where the government from a central point controls and provides solutions for social problems by means of laws and legislations becomes relative immediately. It is more likely that the government will play a facilitating role in the future, certainly in situations where the impact of ICT is characterized by strong differences in sectors, processes and activities.

Developments which will affect the foundations of law most strongly are those of the fading or disappearance of territorial borders, the process of dematerialization and the decline in human intervention. These developments touch the very core of the law; law is very often territory-bound, focussed more or less on concrete physical objects and considers only (legal) persons as possible actors (and not the computer). The process of dematerialization and the declining human intervention make it necessary that numerous concepts within the law are reconsidered. Attention should also be given to the changing societal relationships which involve important consequences for

53. Registratiekamer and Information and Privacy Commissioner/Ontario (1995). Privacy-Enhancing Technologies; the Path to Anonimity. Volume I. Achtergrondstudies en verkenningen 5A; Registratiekamer and Information and Privacy Commissioner/Ontario (1995). Privacy-Enhancing Technologies; The Path to Anonimity. Volume II. Achtergrondstudies en verkenningen 5B.

the law. The employee-employer relationship changes through tele-working, tele-information affects the government-citizen relationship and through tele-shopping the relationship between producer-consumer changes.

In finding solutions, an important problem arises in relation to the fact that they cannot be found within the borders of one country. What is needed is an international approach. Perhaps this could be an approach where the application of the rules is no longer bound to territories but to individuals.

In conclusion, it should be remembered that the indicated inadequacy of the law to adapt quickly to changes requires that the development of new (international) legislation is restricted to basic concepts and rules and does not deal with the numerous – technical – details. The legislature's role as problem solver is relative. In steering and regulating ICT developments emphasis must also be focussed on stimulating and organizing interactions between the various actors in our information society. The formation and implementation of a regulatory policy and the creation of normative frameworks should be the result of (co)production, the actors jointly searching for a strategic compromise. In that event the legislature can act as either actor or director of the compromise. Only such an approach will make our legal system appropriately equipped and sufficiently flexible to deal with the challenges of the 21st century.